

State of Utah
Technical Architecture
Virtual Private Networking (VPN) 2000.08.21

Title: Virtual Private Network Standard

Introduction: VPN services provide the ability to emulate a direct State WAN connection over open public network infrastructures such as ISPs. They also provide the ability to protect data traversing the Internet through data encryption capabilities. VPN technology utilizes a PC based client that connects to a State owned server, which is typically a firewall, or a dedicated VPN server. The initial logon and all data communications between these devices can be fully encrypted to prevent an individual from monitoring the data flow. For smaller installations the Cisco firewall can handle the encryption/de-encryption services with little to no degradation of performance. At larger installations, where a significant amount of encrypted data is required, dedicated VPN servers can be implemented to provide the processing capabilities for the encryption process. Whenever there is sensitive information transferred over an open network such as the Internet, VPN services and encryption are recommended.

Rationale and Justification: Some State Agencies are required by federal law to encrypt their data communications. Where this is necessary VPN solutions can be implemented to meet this mandate. Another factor is the use of State owned IP addresses. When an individual connects to an ISP they are typically assigned an IP number from the ISP address pool. There are some services available on the Internet that are restricted to State owned IP addresses. In this instance, utilizing VPN services would assign a State IP address to the remote individual. This capability allows the remote individual to connect to these sites as though they were directly connected to the State wide area network (WAN). VPN services are an essential component of an overall integrated information security plan that also includes firewalls, PKI, Intrusion Detection, and Web specific security such as SSL, along with general computer security implementations to guard against unauthorized access and attacks. This standard will assist the State in integrating all these capabilities onto a consistent hardware / software platform to maximize business success and security.

Application: This standard is applicable to all executive government agencies in the State of Utah. It also applies to individuals required to conduct business with the State from an IPS or open Internet connection where encryption is required.

Current Architecture: A few agencies have implemented this technology for specific applications, however, there has been no enterprise implementations at present.

Future Architecture: Encryption capabilities are being added to the IP protocol through the IETF standards body. This is known as IPSEC. As these standards are completed and vendors implement this feature in their protocol stacks many of the capabilities of VPN will be resolved. It is important to note that any current or near future implementation of VPN will ultimately be replaced with a standards based IPSEC solution. In other words, Departments need to move cautiously with this technology to avoid multiple rollouts of technology. Where there is an immediate need, this duplication of effort will be required. PKI will also play a direct role with this service as described in the technical considerations section.

Definitions:

IPSEC: IP Security Protocol.

Split Tunnel: The capability of a VPN client to send encrypted traffic through a tunnel and non-encrypted traffic through another path. Particularly beneficial when connecting through an ISP. (The State encrypted traffic can traverse a tunnel to the state, while open Internet traffic will be routed through the ISP and not have to come to the State.)

Tunnel: A direct encrypted dataflow between a VPN client and server.

Authority: Utah Code Section 63D Information Technology Act.

National and International Standards References:

IPSEC - IETF

Technical Consideration(s): With the installed base of Cisco PIX firewalls it is imperative that VPN solutions have tight integration with this environment. As part of the firewall implementation ITS purchased an enterprise license for the Cisco VPN client. This software was marketed by IRE. Cisco recently purchased Altiga, which has its own VPN client. Recently another company was purchased with yet another VPN client. Cisco is consolidating these 4 clients into a new universal client. The specs for this product will not be available until around year-end 2000. These clients are important because each offers some unique capabilities. The IRE client offers multiple concurrent encrypted tunnels along with simultaneous split tunneling. The other clients do not support this capability. However, the IRE client is the most difficult to implement and maintain. Multiple concurrent encrypted tunnels are required by some Departments due to a need to simultaneously access Departmental machines and the ITS mainframe. Where multiple encrypted tunnels are not necessary the Altiga client / sever combination offers a thin client at the desktop that is easily maintained and distributed to remote devices. The Windows 2000 IP stack was co-developed with Cisco and Microsoft and is IPSEC compliant. There has not been enough testing to validate the compatibility between W2K and the Cisco PIX firewall. Agencies requiring VPN services should work closely with ITS to implement a temporary solution that addresses their specific security requirements. The statewide roll out a PKI infrastructure has a direct impact on VPN clients. The VPN software can utilize common PKI authentications. As an example, as an employee is issued a digital certificate as part of the PKI they can use this certificate as a means to validate themselves to the VPN server. The server would then be required to validate the authenticity of the certificate from the PKI provider. Once authenticated, the server would allow the communications through the network. This has obvious ramifications to who can use certificates and how the network authentication will occur. The next layer, or application authentication is not addressed as part of this standard.

Exceptions: There are no authorized exceptions to this standard. However, in the event of a federal mandate, additional VPN products may be implemented on a case-by-case basis.

Gap Analysis: Enterprise VPN clients are available in the form of the IRE client from Cisco or by utilizing W2K. Specific agencies requiring other VPN solutions may identify a need for additional hardware/software. These requirements can be handled by separate projects and budgeting at the Department level. This does not represent a major impact to the WAN.

Approved Configurations: With the purchase of an enterprise license for the Cisco provided IRE VPN client, Departments are encouraged to use this temporary solution. After consulting with ITS, individual Departmental configurations may utilize other Cisco provided solutions to meet the specific agency security requirements.

Migration and Implementation Plan: All new purchases of VPN products will be expected to be in full compliance with this standard.

Review Cycle: This standard will be reviewed and updated on an annual basis, based upon the CIO approval date.

State Purchasing Contracts: Cisco VPN products are available under the following contracts:

Contract Number	Description	Vendor
AR-637	LAN/WAN (US West Router Contract)	Qwest
AR-794	LAN/WAN (US West Switch Contract)	Qwest
AR-877	LAN/WAN Switch Contract	Mountain States Networking

References:

Interim Date: August 21, 2000

Organization Sponsoring the Standard: State Information Security Committee (SISC)

State Technical Architect Approval Date: October 19, 2000

CIO Approval Date: October 19, 2000

ITPSC Presentation Date: October 19, 2000

Author(s): Joe Leary (ITS)